基于隐私保护的实时电价计费方案 *

何 薇 [1a, 1b, 1c]，赵 波 [1a, 1b, 1c]，刘育博 [2]

(1. 武汉大学 a. 计算机学院; b. 空天信息安全与可信计算教育部重点实验室; c. 国家网络安全学院, 武汉 430072; 2. 国网辽宁省电力有限公司 信息通信分公司, 沈阳 110006)

摘　要：针对智能电网基于实时电价的计费过程中有大量实时用电数据需要交互和计算，且隐私数据保护不够完善的安全问题，提出了一种基于隐私保护的实时电价计费方案。利用加法同态加密、混合乘法同态加密等技术，保证了实时用电数据在通信、数据聚合、电费计算和账单验证过程中的安全。同时，通过聚合签名技术减少了数据认证过程中的开销。通过对所述方案进行安全性分析和性能分析，表明该方案具有很好的安全性且性能较高。

关键词：智能电网；实时电价；同态加密；隐私保护；

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2017.12.0823

Real-time pricing scheme based on privacy protection

He Wei[1a, 1b, 1c], Zhao Bo[1a, 1b, 1c], Liu Yubo[2]

(1. *a. School of Computer Science*, *b. Key Laboratory of Aerospace Information Security & Trusted Computing*, *Ministry of Education*, *c. School of National Cybersecurity*, *Wuhan University*, *Wuhan* 430072, *China*; 2. *Information & Communication Branch of State Grid Liaoning Electric Power Company*, *Shenyang* 110006, *China*)

Abstract: Aiming at security problems in smart grid, This paper propose a secure billing scheme based on privacy protection to interact and calculate a large amount of privacy data and improve the privacy data protection. Additive homomorphic encryption and mixed multiplication homomorphic encryption ensure the security of real-time power data in communication, data aggregation, electricity expenditure calculation and billing verification. Meanwhile, the aggregation signature technology has reduced the overhead of data authentication process. The security analysis and performance analysis of the proposed scheme show that the scheme has good security and high performance.

Key words: smart grid; real-time pricing; homomorphic encryption; privacy protection

0　引言

近年来，随着计算、通信、控制等技术的发展，电力系统和信息技术的结合成为了必然的趋势[1]，正是因为两者的有机结合，从而产生了智能电网的概念。智能电网的高速发展对传统固定式电价机制带来了巨大冲击，并由此提出了实时电价策略，将一天分为 24 个时间段甚至更多，每个时段对应不同的电价，实现基于实时价格的电费计算[2]。为了更好地提高资源利用率，达到削峰填谷的效果，电力公司还需要定期收集规定区域内用户总用电量，并综合损耗情况对实时电价进行优化。因此，计费过程中在通信线路上和电费计算阶段有大量的用户实时用电数据需要交互和计算。

实时用电量的交互、计算，为电力公司全面掌握用户的用电情况提供了极大的方便，但也相应带来了严重的隐私安全隐患[3]。正如美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）所指出的[4]，智能电网系统中存在更多更丰富的数据，在带来服务便利的同时，其数据泄露也将带来诸多安全威胁。一旦实时用电信息被攻击者窃取，通过对数据的分析，就能够得到用户详细的家庭生活习惯等方面的信息。因此，智能电网中如何保护用户隐私数据安全成了近年来的研究热点，相关专家学者也做了大量研究。

Lin 等人[5]利用可信计算平台（TPM）和密码技术，设计了可用于账单计算且实现负载均衡的隐私保护系统。刁凤等人[6]提出利用可链接直接匿名认证技术(LDAA)和 Pedersen 承诺构造一个智能电表用户完整隐私保护系统，保证隐私数据在系统内的安全。以上方案都利用了 TPM 对隐私数据进行安全保护，

收稿日期：2017-12-25；**修回日期：**2018-02-16　**基金项目：**国家“863”计划资助项目（2015AA016002）；国家“973”计划资助项目（2014CB340600）

作者简介：何薇（1995-），女，湖北孝感人，硕士研究生，主要研究方向为信息系统安全、网络安全（VianHe@foxmail.com）；赵波（1972-），男，教授，博士，主要研究方向为信息系统安全、网络安全；刘育博（1994-），男，硕士研究生，主要研究方向为信息系统安全、网络安全.**基金项目：**国家 863 高技术研究发展计划（No.2015AA016002）；国家 973 重点基础研究发展计划（No.2014CB340600）.**作者简介：**赵波（1972-），男，教授，博士，主要研究方向为信息系统安全、网络安全，E-mail：zhaobowhu@163.com；何薇，女，硕士研究生.

但因需要额外增加硬件设备，使得系统开销大，实用性较差。

Li 等人[7]提出了基于同态加密的智能电网安全数据聚合方案，利用同态加密的方法保护电量聚合过程中用户的隐私，提出电力公司监控电网运行和预测电力需求所需要的用电数据不需要具体到个人用户的实时用电量。Li 等人[8]提出了一个有效的需求响应方案，该方案实现了电力需求的隐私保护，用户会话密钥的前向安全和私钥更新。Chen 等人[9]以同态加密为基础构造了一种保护用户隐私数据的聚合方案，通过可信第三方为各智能电表和服务器分发相关密钥，在集中器可以得到区域内用电总和的同态加密值。张少敏等人[10]提出利用改进的无证书环签密方案，破坏用户身份和对应用电数据间的关联性以达到隐私保护的目的。由上述文献可知，智能电网中隐私数据的保护方案主要集中在安全数据聚合以及身份匿名方法上，但对实时电价计费过程中隐私数据所面临的安全威胁并未提供有效保护。

本文的主要工作如下：利用加法同态加密、混合乘法同态加密和聚合签名等技术，保护了实时用电信息在数据发送、通信、基于实时电价的电费计算和账单验证全过程中的隐私安全。

与之前的工作相比，本文的优势在于：

a）方案支持基于实时电价的安全计费，保证了计费全过程中的隐私数据安全，符合未来智能电网的发展趋势；

b）方案利用一次实时用电量可同时进行数据融合和电费计算，避免冗余数据，并通过聚合签名的方式减少了通信开销；

c）方案支持动态加入，消息认证，基于用户、控制中心和集中器的多重账单验证等功能，且不需要可信第三方和额外硬件，实用性更高。

1 背景知识

1.1.1 实时电价

因为固定电价无法真正反映用户电力需求和供应之间的关系，在电力需求出现波动时电力公司无法相应的改变电能的供应量，造成大量的资源浪费。对此，提出了实时电价的策略，在考虑运行和基本投资的情况下，在给定时段，如 1 h 或更短时段向用户提供电能的边际成本。通过电价的调节作用，让电力用户自主进行“削峰填谷”，进而提高资源的利用率[11,12]。

1.1.2 聚合签名

聚合签名[13]是一种对多个用户的多个签名进行一次性验证的方法。验证方将从 n 个终端处收集到的 n 个签名进行聚合，只需要对聚合后的签名进行验证，验证通过后即可确定签名是来自指定的 n 个终端。通过聚合签名技术，在缩短了签名长度的同时还减少了验证次数，提高效率。

1.1.3 同态加密

2009 年 IBM 公司的研究员克雷格 •金特里（Craig Gentry）发表了一项密码学的新突破，提出第一个全同态加密方案[14]：利用密钥加密得到密文后，可以直接对密文数据进行代数运算并得到密文结果，对密文结果解密所得的数据和直接对明文进行代数运算所得的数据是相同的。此种方案可在不泄露任何原始数据的前提下，实现数据处理。

同态密码系统中[15]，公钥是 (N,g)，私钥是 λ。$E(\cdot)$，m 和 r 分别为加密函数，明文数据和随机数，对 m 加密即可得到明文 c，如下所示：

$$c = E(m) = g^m \cdot r^N \bmod N^2$$

对密文 c 解密即可得到明文 m，如下所示：

$$m = D(c) = \frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N$$

且 $L(x) = ((x-1))/N$

其中，加法同态特性如下所示：

$$D(E(m_1)\cdot E(m_2) \bmod N^2)$$

$$= D((g^{m_1} \cdot r_1^{\mathrm{N}}) \cdot (g^{m_2} \cdot r_2^{\mathrm{N}}) \bmod \mathrm{N}^2 \bmod \mathrm{N}^2)$$

$$= m_1 + m_2 \bmod \mathrm{N}$$

混合乘法同态特性如下所示：

$$D(E(x)^y \bmod \mathrm{N}^2)$$

$$= D(g^{xy} r^{xy} \bmod \mathrm{N}^2)$$

$$= xy \bmod \mathrm{N}^2$$

2 方案描述

智能电网计费过程中隐私数据所面临的安全威胁主要出现在数据通信和电费计算阶段。智能电表在每个时间段（如 1h）结束后都要向集中器发送一次用电情况，因此在通信过程中有大量的隐私数据需要保护。另外，在电费计算过程中，后台服务器要由实时用电数据和电价计算得到电费值，需要保护服务器中的隐私数据既不会被外部攻击者窃取，也不会因内部员工窥探导致隐私泄露。对此，本文提出了如下的安全方案：

2.1.1 总体方案

智能电表对实时用电数据进行同态加密后将其发送至集中器，集中器利用加法同态和混合乘法同态算法，计算得到当前时段用电量聚合密文值和当日的电费密文并发送至控制中心，控制中心解密可得到聚合电量值和日电费值。其中，同态解密私钥只存在于控制中心，密文计算只在集中器中进行，即通过密文和密钥相分离的方式，不仅保证可在不泄露用电细节的前提下获得总电量和电费，而且还限制了内部员工的权力；在账单验证上，通过用户、控制中心和集中器的三重验证，保证账单的准确性。此外，利用签名融合技术实现一次验签，在保证源安全的同时又提高了效率。

网络拓扑结构如图 1 所示，其由域、智能电表、集中器、控制中心和客户端组成。具体介绍如下：

a）域（R）。以地理位置、电表数量等为依据划分，一个域对应一对同态公私钥，域内包含 m 个智能电表。

b）智能电表（SM）。安装在用户侧的终端设备，具有收集、上传用电数据的功能，内置注册阶段所需的加密密钥。

c）集中器（LAG）。智能电表和电网后台服务器的桥梁，具有接收、存储、转发和计算等功能，一个域对应一个集中器；

d）控制中心（CC）。具备一定的运算、存储能力，负责密钥的生成、更新、分发以及电价表的制定和更新。

e）客户端（Client）。服务于用户，由客户端程序实现用电清单查询。

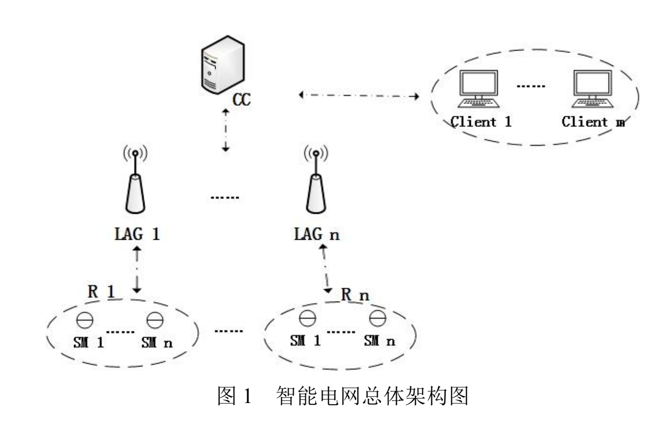


图 1 智能电网总体架构图

2.2 方案流程

2.2.1 初始化

该阶段主要由控制中心生成聚合签名算法[16]和同态加密算法所需的相关参数，具体步骤如下：

a)控制中心生成与聚合签名算法相关的密钥参数，包括大素数 q，阶为 q 的加法循环群 G_1,G_2，阶为 q 的乘法循环群 G_T，群 G_1,G_2 的生成元 a_1,a_2， 双线性映射 $e:G_1\times G_2\rightarrow G_T$；

b)控制中心以 $s\in Z_p^*$ 作为系统主密钥，计算系统公钥 y；

$$y=g_2^s$$

c) 控制中心选择两个 $Hash$ 函数：$H_1(\cdot):\{0,1\}^*\rightarrow G_1;H_2(\cdot):\{0,1\}^n\rightarrow G_2$，同时公布相应的系统参数以供查阅；

$$\text{params}=\{q,G_1,G_2,G_T,a_1,a_2,e,s,y,H_1,H_2\}$$

d)控制中心为同态加密算法设定一种安全级别参数 k，选择大素数 p，且 $|p|=|q|=k$，分别计算 $n=pq,\lambda=lcm(p-1,q-1)$；

e)控制中心选取随机数 x_u 和 d_u，计算签名私钥 Pri_u 和公钥 Pub_u： $Pri_u=x_usH_1(d_u)$，$Pub_u=<X_u,Y_u>,X_u=x_ua_1,Y_u=x_ua_1s$。

2.2.2 电表注册

该阶段主要实现智能电表的激活、注册认证以及相关密钥参数的安全分发，具体步骤如下：

a)用户或开发商向电力公司申请电表入户，电力公司审核通过后为智能电表写入唯一的识别码 ID_{SM_i} 和由随机数发生器生成的内置密钥 K_o。电力公司根据申请地的位置信息将智能电表安装并设置至所属域中，同时将 ID_{SM_i}、K_o 和 Pri_u 发送至集中器，将 K_o 和 Pub_u 发送至控制中心；

b)智能电表生成激活请求信息，包括电表标志 ID_{SM_i} 和时间戳 TS，利用内置密钥 K_o 加密并发送至集中器。集中器解密后，判断 ID_{SM_i} 是否属于该集中器，若 ID_{SM_i} 和集中器中数据匹配，则返回成功标志。否则，将发送者的 ip 地址暂时隔离，拒收其后续信息，并由后台服务器做进一步审核，判断是否为恶意攻击；

c)智能电表收到激活成功标志后，生成特定格式的注册消息 R_S，包括电表标志 ID_{SM_i}、用户标志 ID_{UR_i}、位置信息 $loinfo$ 和用户信息 $uinfo$，利用内置密钥 K_o 加密得到 C_s，同时利用哈希算法计算得到 R_s 和 K_o 的摘要值 Dig，将注册标志 Reg、C_s 和 Dig 作为注册请求 Req 一起发送至对应的集中器；

$$C_s=Enc_{k_o}\left(ID_{SM_i},ID_{UR_i},loinfo,uinfo\right)$$

$$Dig=H_1\left(R_s,K_0\right)$$

$$Req=Reg|C_s|Dig$$

d)集中器将该注册请求 Req 利用签名私钥 Pri_u 签名，并转发至控制中心；

e)控制中心利用公钥 Pub_u 验签，若验签失败则返回错误信息；否则，控制中心利用 K_o 解密并验证摘要值，验证通过后，利用发送的 ID_{SM_i} 值生成智能电表的签名私钥 k_s；

$$ID_{SM_{i,0}}=H_1\left(ID_{SM_i},0\right),$$

$$ID_{SM_{i,1}}=H_1\left(ID_{SM_i},1\right)$$

$$k_{i,0}=ID^s_{SM_{i,0}},$$

$$k_{i,1}=ID^s_{SM_{i,1}}$$

$$k_s=(k_{i,0},k_{i,1})$$

f)控制中心将注册消息 R_S、系统参数 $params$、电表私钥 k_s、有效期 VP 连同其摘要值 MAC 一同利用 K_o 加密发送至集中器，集中器解密后将 ID_{SM_i}、ID_{UR_i}、$loinfo$、$uinfo$ 存储在注册表中，完成电表注册；

$$MAC=H_1\left(R_S,params,k_s,VP\right)$$

$$Enc_{k_o}\left(R_S,params,k_s,MAC\right)$$

g)集中器转发 $params,VP$ 和 k_s 至对应的智能电表，智能电表解密得到相关参数、有效期及私钥并保存，同时记下当前时间，当使用时长超过有效期 VP 时，由智能电表向控制中心发送维护申请，更新密钥信息。

2.2.3 数据发送

设当前时段为 t，每个时段 1h，即电价表由 24 个时段电价值组成。集中器中存有电价表、最新更新时间 t_s 和电价表更新周期 ut，数据发送阶段的具体流程如下：

a)集中器首先判断电价表是否失效，若 $t-t_s>ut$ 则电价表已失效，需要向控制中心发送更新请求。控制中心返回更新后的 24 个时段的电价，集中器将新电价值写入电价表，并记录当前时间作为最新更新时间 t_s。若未失效则继续执行后续步骤；

b)在当前时段结束后，智能电表生成由电表标志 ID_{SM_i}、当

前时段 t 和时间戳 TS 构成的验证信息，并利用内置密钥 K_o 加密后发送至集中器。集中器验证该电表是否属于所在域且 t 是否为当前时段值，若匹配则返回验证成功标志，否则将该设备暂时隔离，禁止其继续向集中器发送信息，防止恶意攻击；

c)智能电表收到成功标志后，将该时段内的用电量 P_t，利用同态公钥进行加法同态加密得到电量密文 $E(P_t)$，同时利用电表身份 ID_{SM_i} 和初始化阶段生成的私钥 k_s 对该电表 ID_{SM_i} 在时段 t 内的电量密文 $P_{i,t}$ 进行签名；

$$E(P_t)=g^{P_t}r^n$$

$$\sigma_{i,t}\left(\mathrm{E}\left(P_{i,t}\right)\right)=k_{i,0}k_{i,1}^{\;h_{i,t}}$$

其中，$h_{i,t}=H_2\left(\mathrm{E}\left(P_{i,t}\right),ID_{SM_i}\right)$

d)随机选择数字 r（$1\le r\le 15$），在当前时段结束并再过 r 分钟后，将相关数据发送到集中器中，其中 TS 为时间戳；并将相关信息存储在电量密文表中，如表 1 所示。

$$ID_{SM_i}\left|E\left(P_{i,t}\right)\right|s_{i,t}\left(E\left(P_{i,t}\right)\right)|TS$$

表 1　电量密文表

电表标识	时段	电量密文
ID_{SM_1}	t_1	$E\left(P_{1,t1}\right)$
ID_{SM_2}	t_1	$E\left(P_{2,t1}\right)$
ID_{SM_3}	t_1	$E\left(P_{3,t1}\right)$

2.2.4 电费计算

利用加法同态加密和混合乘法同态加密算法，在集中器中由电量密文和实时电价计算得到电量聚合密文和日电费密文，控制中心中解密可得到相应结果值。同态解密密钥只存在于控制中心，集中器没有密钥无法解密，只能实现对密文的计算。即在集中器中只有隐私数据密文，在控制中心中只有明文结果值。保证可以在不泄露用户隐私的前提下获得用电总量和电费值，保护了用户隐私数据安全。此外，通过聚合签名技术，在验证数据源的同时减少通信、计算开销，具体过程如图 2 所示。

a)集中器收到智能电表发送来的电量密文后，对本域内 m 个智能电表发来的签名值进行聚合得到 ξ_t，之后利用加法同态算法得到电量聚合密文值 Tol_t；

$$\xi_t=\prod_{i=1}^{m}\sigma_{i,t}$$

$$Tol_t=\prod_{i=1}^{m}E\left(P_{i,t}\right)=\prod_{i=1}^{m}g^{p_{i,t}+p_{i+1,t}\cdots\cdots p_{s_m,t}}\cdot \mathrm{r}^{\mathrm{n}}\bmod n$$

b)在集中器中由电量密文和单价利用混合乘法同态算法计算得到日电费密文值 Cha_t；

$$Cha_t=\sum_{i=1}^{24}E\left(P_i\right)\times C_i=\sum_{i=1}^{24}E\left(P_i\right)^{C_i}\bmod n^2$$
$$=\sum_{i=1}^{24}\left(g^{P_i}r^n\right)^{C_i}\bmod n^2=\sum_{i=1}^{24}g^{p_ic_i}r^{nc_i}\bmod n^2$$

c)各集中器将融合后的签名值、聚合密文、电费密文以及时间戳发送至控制中心；

$$ID_i\,|\,Tol_t\,|\,Cha_t\,|\,\xi_t\,|\,TS$$

d)控制中心验签，首先计算验证所需的相关参数；

$$h_{i,t}=H_2\left(E\left(P_{i,t}\right),ID_{i,t}\right)$$

$$ID_{i,t,0}=H_1\left(ID_{i,t},0\right)$$

$$ID_{i,t,1}=H_1\left(ID_{i,t},1\right)$$

随后验证等式，若不成立则聚合签名验证失败；

$$e\left(\xi_t,g_2\right)=e\left(\prod_{i=1}^{m}(ID_{i,t,0}\cdot ID_{i,t,1}^{\;h_{s_i,t}}),y\right)$$

e)聚合签名验证成功后，控制中心利用智能电表所在群的同态私钥解密，即可在并不知道用户具体用电情况的前提下得到各用户在当前计费周期的电费明文 $\mathrm{M}_{i,t}$ 和聚合数据明文 T_t；

$$M_{i,t}=D\left(Cha_t\right)=\frac{L(Cha_t^{\;\lambda}\bmod n^2)}{L(g^{\lambda}\bmod n^2)}\bmod n$$
$$=\sum_{i=1}^{24}p_i\times c_i$$

$$T_t=D\left(Tol_t\right)=\frac{L(Tol_t^{\;\lambda}\bmod N^2)}{L(g^{\lambda}\bmod N^2)}\bmod N$$
$$=\sum_{i=1}^{m}p_i$$

且 $L\left(x\right)=\left(\left(x-1\right)\right)/N$

f)将用电总和反馈至后台服务器，实现后续的电价制定；将电费值反馈至营销服务器，扣费，计费过程完成。

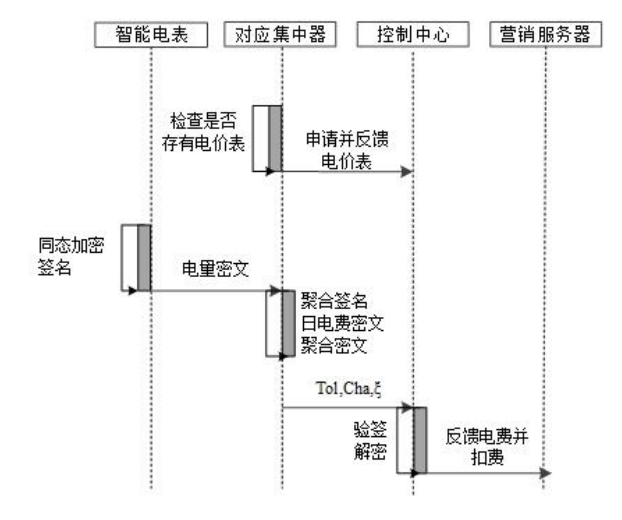


图 2　电费计算流程图

2.2.5 账单验证

由用户、控制中心和集中器实现对账单的多重认证，先申请再解密，集中器仅需返回特定的用电明细明文，最大程度保证隐私数据的安全，具体过程如图 3 所示。

a)用户通过客户端输入登录名和密码，登录成功后，选择想要申请验证的计费周期，即可生成包括电表 ID、起始时间 $stime$、终止时间 $etime$ 和时间戳等特定格式的验证申请信息，并将其发送至控制中心；

$$ID_{SM} \mid stime \mid etime \mid TS$$

b)控制中心首先验证用户身份。若验证不通过则返回错误信息。若成功，则将起始和终止时间值发送至集中器，并在集中器的电量密文表中首先利用电表标志 ID_{SM} 筛选该电表对应的条目，随后通过日期值确定条目范围，将该电表 ID 值，所属域的域标志 $area$，范围内的电量密文和对应的时段信息发送至控制中心；

$$\text{for}(ID_{SM} = ID_{SM}'; stime <= etime; stime++)$$

$$ID_{SM} \left| area \right| elec\left[s_{time} \right] \mid time \mid TS$$

c)控制中心通过域标志确定所属域私钥并用私钥解密，从而获得各时间段内的用电量明文，重新计算电费值 M' 判断是否与自身存储的电费值 M 相等，若相等则将用电量明文细节反馈至对应用户的客户端中；

$$M' = \sum_{i=1}^{etime-stime} p_i \times c_i$$

d)客户端根据各时间段信息、用电量并结合公布的各时段电价，即可生成在特定范围内的用电清单供用户查阅，实现账单验证。

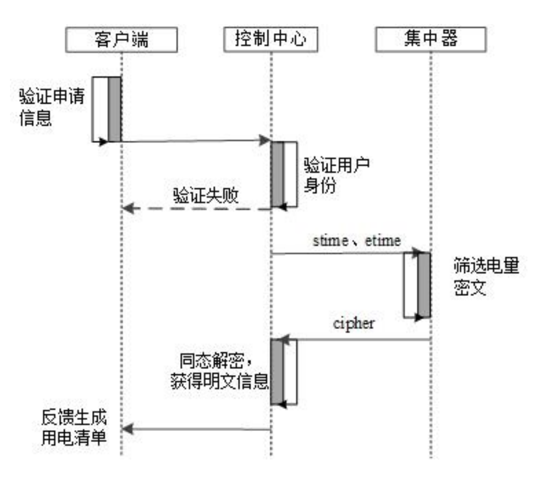


图 3 电费验证流程图

3 系统性能分析

3.1 安全性分析

首先，对本方案所达到的安全目标进行分析。

3.1.1 数据源认证

智能电表在与对应的集中器进行通信之前，先进行设备的注册，在注册时，需要利用智能电表中的内置密钥加密电表 ID、位置等信息发送至集中器中，集中器解密后将信息写入对应的信息表中。保证其他设备无法伪造该设备的注册操作，且只有智能电表的身份验证通过后才能与集中器进行通信，证明消息来源的可靠性。

此外，在智能电表和控制中心通信时，智能电表对密文信息进行签名并发送至集中器，集中器对签名融合后转发至控制中心，控制中心验签，保证身份合法。

3.1.2 数据的机密性与完整性

计费时，在通信信道和集中器中的用户用电数据都是密文，只在控制中心可以得到明文，其他组成部分都无法解密获取明文信息，保证即使攻击者窃取到通信信息，也无法得到任何涉及用户隐私的用电量数据信息等。

此外，在方案的多个关键环节中，需要生成特定格式的注册或验证请求，在请求中需要加入对相关信息进行摘要得到的消息认证码，只有在服务器端验证通过后才接收该值，保证了相关信息数据的完整性并防止窜改。

3.1.3 细粒度隐私数据保护

控制中心接收到的密文数据，都是各个集中器对域内所有的智能电表电量密文和电价计算后的电费密文值或聚合密文值，无法拆分得到各用户的用电细节。在电费计算过程中利用同态加密技术，确保仅在安全的控制中心拥有密钥可以解密得到计算后的明文电费，在智能电表和集中器等非安全区和通信信道中都是加密后的用电细节且没有解密密钥，采用隐私密文和密钥相分离的方式，防止外部攻击导致数据被窃取的同时也限制了内部员工的权力，对隐私数据实现细粒度的安全保护。在账单验证过程中，实现了多重账单验证，在客户端采用先申请再解密的方式，仅需返回必要的明文即可生成用电清单，在最大程度上防止了用户隐私数据的泄露。扩大了系统的安全范围，安全性较高。

3.2 功能性分析

其次，对本文方案所具备的功能进行说明。

a)动态用户。在新电表申请加入时，智能电表仅需与控制中心进行交互，由控制中心分发相关密钥、存储电表基本信息并将电表设定至相应的域即可完成动态用户的加入，过程中不需初始化所有配置信息。当某个电表因故障需要退出时，在集中器中将该电表的信息标记为故障即可将其撤销。

b)实时电价计费。在通常的电费计算方案中，支持的多为阶梯式电价计费方案，以用户在一个较长时间段内的用电量作为计算值，通过阶梯计费的方式计算用户电费，然而该方法并不适用于实时电价策略。在本文提出的电费计算方案中，设一天包含 k 个时间段，智能电表在当前时间段结束后即向集中器发送当前时段的用电量密文，控制中心将该时段电价值反馈至集中器和电表中。集中器根据该时段的单价值即可根据混合乘法同态算法计算出当前时段内的电费值密文，以此类推计算 k 次可得当日的电费密文，反馈至控制中心得到日电费值。

c)数据聚合。为了更好地提高资源利用率，智能电网需要

实时掌握区域内的用电量总值，从而达到削峰填谷的效果。智能电表每隔 1 h 或更短向集中器发送一次本时间段内的实时用电量密文，集中器对域内密文做同态加法即可得到域内电表在该时段内的用电量密文。以此类推，在控制中心对所有域的域内用电量密文相加即可在不泄露具体用户用电细节的前提下得到用电量总值。仅需一次数据传输，即可同时分别完成数据聚合操作和电费计算过程，减少了额外的通信开销。

d)账单验证。本文方案在账单验证上增加了用户因素，当用户对反馈的电费值提出异议时，通过先申请再解密的方式，由客户端向控制中心发出验证申请，控制中心将待查询用电量的开始时间和结束时间发送至对应集中器。集中器将电量密文返回后，控制中心解密并根据电价表重新计算电费值 M'，比较原电费存有值 M 是否与相等，通过对用户、集中器和控制中心的三重比对，保证电费计算的可靠。同时，将各时段电量值返回至客户端，以便用户实现清单查询。

表 2　不同方案的功能对比

方案	存在TTP	聚合签名	实时电价计费	多重账单认证	同步聚合计算
[6]	No	No	No	No	No
[8]	No	Yes	No	No	No
[9]	Yes	Yes	No	No	No
[10]	Yes	No	No	No	Yes
本文	No	Yes	Yes	Yes	Yes

在表 2 中给出了其他方案和本方案在功能性上的比较分析。通过比较发现，本方案具有的功能更全面，基于实时电价的电费计算方法更符合未来智能电网的发展趋势；仅提取一次数据可同步实现数据聚合和电费计算，且通过聚合签名验证来源，通信开销更小；采用多重账单认证，准确性更高；方案不需要可信第三方，实用性更高。

3.3　效率分析

本节详细分析了电费计算过程中各终端的计算开销和通信开销。

1）计算开销

在计算开销上，分别从智能电表、集中器和控制中心进行分析，将本文所述电费计算方案与利用同态加密方法实现数据聚合的 EPPA 方案[15]进行对比，结果如表 3 所示。

本文提出的电费计算方案的计算开销主要包括哈希运算 T_{MTP}、同态加密运算 T_E、同态解密运算 T_D、签名算法中的指数运算 T_{exp}、签名算法中的乘法运算 T_{mul} 和双线性对运算 T_{par}。其中最主要影响时间开销的为同态加解密运算和双线性对运算，其他运算的时间开销都较小可忽略不计。设一个集中器中包含 m 个智能电表，一天包含 k 个时段。

由表 3 可知，在 SM 处，两者的计算开销几乎相同；在 LAG 处，本文方案计算开销小于 EPPA；在 CC 处，本文方案计算开销略大于 EPPA。对比可知，本文所述电费计算方案并未增加过多计算开销，可以适用于智能电网系统。

表 3　计算开销对比

	SM	LAG	CC
电费计算	$T_E + T_{MTP} + T_{exp} + T_{mul}$	$((k+1)m-1)T_{mul} + kmT_{exp}$	$T_D + 2T_{par} + 3mT_{MTP} + (2m-1)T_{mul} + mT_{exp}$
EPPA	$T_E + T_{MTP} + T_{exp}$	$(m+1)T_{par} + mT_{MTP} + (m-1)T_{mul}$	$T_D + 2T_{par} + T_{MTP}$

2）通信开销

本文所述电费计算方案的通信开销主要是指为完成既定方案在系统中需要额外增加的通信数据量。设同态加密中的 n 的值为 512 bit，群 G_1 元素的长为 171 bit，ID 值的长度为 32 bit，时间戳 TS 为 32 bit。

智能电表需要发送的数据为智能电表的 ID 值，该时段的电量密文值，聚合签名值和时间戳，即长度为 32+1024+171+32=1259 bit。通信开销较小。

通过评估，可以证明本文所述的电费计算方案能很好的适用于智能电网系统，性能和实用性较好。

4　结束语

本文提出了一种基于隐私保护的智能电网安全计费方案，分别保证了用户实时用电数据在通信、电费计算和账单验证等过程中的隐私安全。方案支持基于实时电价的电费计算，符合未来智能电网的发展趋势；方案仅提取一次实时用电数据可以实现数据聚合和账单计算，减少了冗余数据，而且通过聚合签名的方式在批量验证数据来源的同时也降低了计算、通信开销；引入用户因素实现多重账单认证，可靠性更高。通过安全性分析和性能分析，证明该方案具有较好的安全性和可行性且性能较高，具有很好的应用价值和现实意义。

参考文献：

[1] Gungor V C, Sahin D, Kocak T, *et al.* Smart grid technologies: communication technologies and standards [J]. IEEE Trans on Industrial Informatics, 2011, 7 (4): 529-539.

[2] Allcott H. Rethinking real-time electricity pricing [J]. Resource & Energy Economics, 2011, 33 (4): 820-842.

[3] 黄秀丽, 张涛, 马媛媛, 等. 智能电网隐私保护技术的分析研究 [J]. 计算机技术与发展, 2014 (2): 189-193.

[4] Harvey M, Long D, Reinhard K. Visualizing NISTIR 7628, guidelines for smart grid cyber security [C]// Proc of Power and Energy Conference at Illinois. 2014: 1-8.

[5] Lin H Y, Tzeng W G, Shen S T, *et al.* A practical smart metering system supporting privacy preserving billing and load monitoring [C]// Applied Cryptography and Network Security. Berlin: Springer, 2012: 544–560.

[6] 刁凤, 张方国. 智能电表的完整隐私保护系统 [J]. 密码学报, 2014, 1 (4): 400-409.

[7] Li F, Luo B, Liu P. Secure information aggregation for smart grids using homomorphic encryption [C]// Proc of the 1st IEEE

[8] International Conference on Smart Grid Communications. 2010: 327–332.

[9] Li H, Lin X, Yang H, *et al.* EPPDR: an efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid [J]. IEEE Trans on Parallel & Distributed Systems, 2014, 25 (8): 2053-2064.

[10] Chen L, Lu R, Cao Z, *et al.* MuDA: multifunctional data aggregation in privacy-preserving smart grid communications [J]. Peer-to-Peer Networking and Applications, 2015, 8 (5): 777-792.

[11] 张少敏, 赵乙桥, 王保义. 智能电网下保护用户隐私的无证书环签密方案 [J]. 电力系统自动化, 2018 (3): 1-7.

[12] 殷树刚, 张宇, 拜克明. 基于实时电价的智能用电系统 [J]. 电网技术, 2009 (19): 11-16.

[13] 周玲芳. 智能电网条件下的用户侧实时电价机制研究 [D]. 北京: 华北电力大学, 2015.

[14] Boneh D, Gentry C, Lynn B, *et al.* Aggregate and verifiably encrypted signatures from bilinear maps [C]// Lecture Notes in Computer Science, vol 2656. 2003: 416-432.

[15] Gentry C. Fully homomorphic encryption using ideal lattices [C]// Proc of the 41st Annual ACM International Symposium on Theory of Computing. 2009: 169-178.

[16] Lu R, Liang X, Li X, *et al.* EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications [J]. IEEE Trans on Parallel and Distributed Systems, 2012, 23 (9): 1621-1631.

[17] Zhang L, Wu Q, Qin B, *et al.* APPA: aggregate privacy-preserving authentication in vehicular Ad hoc networks [M]// Information Security. [S. l.] : Springer Berlin Heidelberg, 2011: 293-308.